APPLICATION SANDBOXING

PRINCIPLES, TECHNOLOGIES, AND SECURE ISOLATION

- NAMESPACES & CGROUPS
- CONTAINERS
- VM VIRTUAL MACHINES
- µVM MICROVMS
- WA WEBASSEMBLY
- BROWSER SANDBOXES
- CONFIDENTIAL COMPUTING

ISOLATED EXECUTION | MINIMAL ATTACK SURFACE | PRIVILEGE BOUNDARIES | AUDITABLE & CONTAINED

STEVE T.

Application Sandboxing

Principles, Technologies, and Secure Isolation

Steve T. Team Publications

This book is available at https://leanpub.com/applicationsandboxing

This version was published on 2026-07-03

Contents

Principles, Technologies, and Secure Isolation

About this book: This book is a comprehensive technical guide to application sandboxing in modern computing. It covers the theory, architecture, implementation, and security models behind every major isolation technology, from Linux namespaces and cgroups through containers, virtual machines, microVMs, WebAssembly, browser sandboxes, and confidential computing. You will learn how each approach works under the hood, what trade-offs it makes in security versus performance versus portability, how attackers bypass these boundaries, and how to select, implement, and harden sandboxing solutions for desktop, server, cloud-native, and embedded environments. Whether you are a systems engineer designing the next generation of secure infrastructure, a security professional hunting for escape vectors, or an application developer who needs to ship code that runs safely in shared environments, this book will give you the technical depth and practical guidance to make informed decisions about isolation.

Introduction: When Isolation Fails

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

The Promise of Sandboxing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

What This Book Covers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

What This Book Does Not Cover

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

How to Read This Book

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

A Note on the Evolving Landscape

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Chapter 1: Why Sandboxing? — The Threat Model and the Promise of Isolation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

The Cost of Unbounded Execution: Real Incidents

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Blast Radius and the Defense-in-Depth Philosophy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

A Taxonomy of Isolation Mechanisms

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

What This Book Will (and Won't) Cover

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Chapter 2: The Kernel as Enforcer — Namespaces, Cgroups, and the Linux Sandboxing Stack

Namespaces: Partitioning What You See

Cgroups: Controlling What You Can Do

User Namespaces and Unprivileged Containers

Composing Isolation: From Primitives to Containers

Limitations and Known Gaps in Linux Isolation

Chapter 3: Mandatory Access Control — SELinux, AppArmor, and Smack

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Discretionary vs Mandatory Access Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

SELinux: Architecture and Policy Model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

AppArmor: Profile-Based Protection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Smack and Alternative MAC Frameworks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Operational Challenges and Adoption Barriers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Chapter 4: System Call Filtering — seccomp, Landlock, and Capability Dropping

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Linux Capabilities: Fine-Grained Privilege Splitting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

seccomp-bpf: Filtering the System Call Surface

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Landlock: A New Era of Unprivileged Sandboxing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Composing Filters with Capability Dropping

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Real-World seccomp Profiles and Case Studies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Chapter 5: eBPF — The Universal Sandbox Primitive

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

From TCPdump to Trusted Kernel Runtime: The eBPF Revolution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

How eBPF Works: Verifier, Programs, and Maps

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

eBPF for Network and Filesystem Sandboxing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Observability-Driven Security with eBPF

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Trust Boundaries and the eBPF Threat Model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

The eBPF Security Model in Practice

Chapter 6: Container Runtimes and the OCI Ecosystem

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

The OCI Standard: Making Containers Portable

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Docker Architecture Deep Dive

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

containerd and CRI-O: Kubernetes-Native Runtimes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Rootless Containers and User Namespace Remapping

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Storage Drivers and Image Layers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Chapter 7: Virtual Machines and MicroVMs — Hardware-Level Isolation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Virtualization Fundamentals and the Hypervisor Stack

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

KVM and QEMU: The Linux Virtualization Foundation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

MicroVMs: Firecracker, Crosvm, and the Edge of Performance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Security Comparison: VMs vs Containers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

When to Choose Hardware Isolation Over OS-Level Sandboxing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Chapter 8: Desktop and Mobile Sandboxes — macOS, Windows, Android, iOS, and Browsers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

macOS Sandbox: Seatbelt and Entitlements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Windows AppContainer and Virtual-Based Sandboxing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Android's Per-App Isolation Model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

iOS Application Sandboxing and Entitlements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Browser Sandboxes: Process Isolation and Site Separation

Chapter 9: Language and Runtime Sandboxes — From chroot to WebAssembly

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

chroot: The Oldest Trick in the Book

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

FreeBSD Jails: BSD's Isolation Philosophy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

LXC and LXD: System Containers on Linux

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

WebAssembly and WASI: Sandboxing at the Bytecode Level

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Language and Runtime Sandboxing Approaches

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Chapter 10: Sandbox Escapes — How Isolation Fails and What to Do About It

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Container Escape Techniques and Case Studies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

VM Escape: Hypervisor Vulnerabilities and Side Channels

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Browser Sandbox Bypasses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Desktop OS Sandbox Escapes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Defense Strategies and the Ongoing Arms Race

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Chapter 11: Designing and Operating Sandboxed Environments

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Threat Modeling Your Sandboxing Strategy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Selecting Isolation Technology for Different Workloads

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Hardening Container Images and Runtimes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Network Segmentation and Zero-Trust Networking

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Observability, Debugging, and Operational Excellence

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Chapter 12: The Future of Sandboxing — Serverless, Confidential Computing, and Beyond

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Serverless Isolation: The Function-as-a-Service Model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Confidential Computing: When the Kernel Can't Be Trusted

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

WebAssembly's Expanding Sandbox Horizon

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

The Convergence Playbook: Containers, VMs, and Wasm Together

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.

Open Challenges and Where the Field Is Heading

Conclusion: The Principle of Measured Trust

References

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/applicationsandboxing.